(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－82834
（P2002－82834A）
(43)公開日　平成14年３月22日(2002.3.22)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
G06F	12/14	320	G06F	12/14	320A　5B017
	11/34			11/34	C　5B035
G06K	19/00		G09C	1/00	640B　5B042
	19/10		G06K	19/00	Q　5J104
G09C	1/00	640			R

審査請求　未請求　請求項の数６　ＯＬ　（全 14 頁）

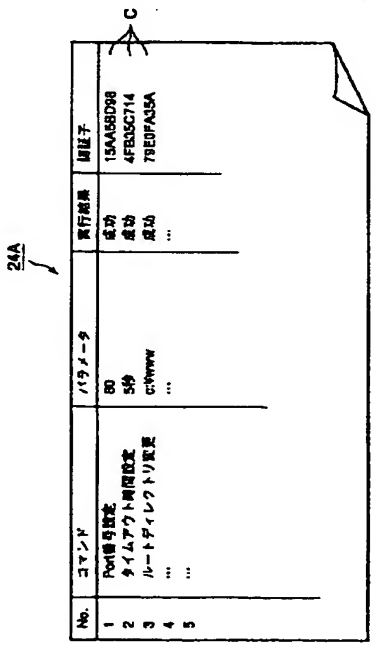
(21)出願番号　特願2000－271904(P2000－271904)
(22)出願日　平成12年９月７日(2000.9.7)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　西澤　秀和
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(72)発明者　加藤　岳久
東京都府中市東芝町１番地　株式会社東芝府中事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　履歴管理用の記憶媒体及びＩＣカード

(57)【要約】
【課題】　管理者による履歴の改ざんを阻止する。
【解決手段】　管理者の操作履歴に対して各履歴データ毎に認証子Ｃをつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性とを保証する。また、最新の認証子Ｃの比較結果をも検証するので、最新の履歴データが削除されていない旨をも保証する。



【特許請求の範囲】
【請求項１】　計算機システムの操作の履歴管理を実現するための履歴管理用のコンピュータ読取り可能な記憶媒体であって、
前記計算機システムのコンピュータを、
前記操作毎に今回の履歴データ及び認証子が追加的に記憶される履歴テーブルを形成するテーブル形成手段、
前記操作毎に今回の履歴データ及び前回の認証子に基づいて今回の認証子が生成されると、この今回の認証子を前記今回の履歴データと組にして前記履歴テーブルに記憶させる履歴管理手段、
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。
【請求項２】　請求項１に記載のコンピュータ読取り可能な記憶媒体において、
前記計算機システムのコンピュータを、
前記履歴テーブル内の各回の履歴データ毎に、当該回の履歴データと当該回の前回の認証子とに基づいて、当該回の認証子が生成されるか否かを定期的に検証する第１の検証手段、
前記第２の検証手段により当該回の認証子が生成されないとき、警告を発する第１の警告手段、
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。
【請求項３】　請求項２に記載のコンピュータ読取り可能な記憶媒体において、
前記計算機システムのコンピュータを、
前記履歴テーブル内の最新の認証子を比較のために出力し、折り返し入力された比較結果を判定する第２の検証手段、
前記第２の検証手段による判定結果が不整合を示すとき、警告を発する第２の警告手段、
として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体。
【請求項４】　請求項３に記載のコンピュータ読取り可能な記憶媒体において、
前記第２の検証手段は、ログオンのときに動作することを特徴とするコンピュータ読取り可能な記憶媒体。
【請求項５】　電子計算機システムの操作の履歴管理を実現するための履歴管理用のＩＣカードであって、
耐タンパー性を有し、最新の認証子が記憶される最新認証子記憶手段と、
前記操作毎に今回の履歴データが入力されると、今回の履歴データと前記最新認証子記憶手段内の最新の認証子とに基づいて、今回の認証子を生成する認証子生成手段と、
この認証子生成手段により生成された今回の認証子を最新の認証子として前記最新認証子記憶手段に書込む認証子書込手段と、
認証子が入力されたとき、この入力された認証子と、前記最新認証子記憶手段内の最新の認証子とを比較し、比較結果を出力する認証子比較手段と、
を備えたことを特徴とするＩＣカード。
【請求項６】　請求項５に記載のＩＣカードにおいて、
パスワードによる操作者の認証を実行する操作者認証手段を備え、
前記認証子比較手段は、前記操作者認証手段による認証結果が正当なとき、動作することを特徴とするＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、計算機システムの操作の履歴管理を実現するための履歴管理用の記憶媒体及びＩＣカードに係り、特に、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びＩＣカードに関する。
【０００２】
【従来の技術】従来、計算機システムでは、個人のファイルの覗き見又は改変等の不正アクセスや、ネットワーク設定等の不正な改変といった様々な不正操作を阻止する観点から、履歴管理用のプログラムがインストールされて実行されている。図１４はこの種の計算機システムの概略を示す模式図であり、図１５はこの計算機システムの構成を示す機能ブロック図である。
【０００３】この計算機システムは、計算機１０とサーバ装置２０とがネットワークＮＷを介して接続され、サーバ装置２０には管理操作用のコンソール１０＊が接続されている。但し、コンソール１０＊と計算機１０とは基本的に同一構成であり、ネットワークを介するか否かの違いしかないので、以後の説明では、コンソール１０＊からの管理操作の記載を省略し、計算機１０からの管理操作を例に挙げて述べる。
【０００４】一般に、計算機１０は任意の部屋に設置されるが、サーバ装置２０は、物理的な脅威から保護されるように、計算機１０の部屋とは異なる安全な部屋に設置される。システム管理者は、システムの全操作を実行可能な権限を有し、計算機１０をネットワークＮＷ経由でサーバ装置２０に接続して管理操作を行なう。
【０００５】ここで、計算機１０は、例えばパーソナルコンピュータ（ＰＣ）等が使用可能であり、サーバ装置２０のソフトウェアを遠隔管理するための管理ソフトウェアがインストールされている。計算機１０は、具体的には図１５に示すように、システム管理者の管理操作用の視覚的ツールであるＧＵＩ(Graphical User Interface)１１と、システム管理者によるＧＵＩ１１の操作に基づき管理用のコマンド電文を作成するコマンド発行機能１２と、この作成されたコマンド電文をネットワークＮＷ経由でサーバ装置２０に送出するソケット１３とがインストールされている。
【０００６】サーバ装置２０は、サービスを提供するソ

フトウェアがインストールされて稼働しており、具体的には、計算機１０からのコマンド電文を受け取るソケット２１と、この受け取ったコマンド電文を解釈するコマンド解釈機能２２と、コマンド電文を解釈したコマンド解釈機能２２に制御され、サーバ装置２０の各種の管理をコマンド電文に応じて個別に実行する複数の管理機能２３（Ａ，Ｂ，Ｃ，…）とがインストールされ、コマンド解釈機能２２により、管理機能２３にて実行された管理操作の履歴が記録される履歴テーブル２４が形成されて使用されている。

【０００７】ここで、履歴テーブル２４は、図１６に一例を示すように、個々の管理操作（コマンド電文）に対応して各行毎に、Ｎｏ．（連番の番号）、コマンド（操作内容）、パラメータ及び実行結果（成功又は失敗）が記録された表形式の記憶領域である。この履歴テーブル２４の参照により、システム管理者による管理操作は、その実行順序に沿って履歴管理されている。

【０００８】

【発明が解決しようとする課題】しかしながら以上のような履歴管理では、第三者に対しては不正操作の痕跡を記録することから不正操作を阻止し得るものの、システム管理者に対しては不正操作の痕跡が消去可能であることから不正操作を阻止し得ない状況にある。

【０００９】詳しくは、システム管理者は、計算機システムの全操作の権限を持つため、不正操作が履歴テーブル２４に記録されても、自己の操作権限により、履歴テーブル２４を改ざんして不正操作の痕跡を消去可能であるからである。

【００１０】なお、履歴テーブル２４の改ざん内容としては、次の（１）～（５）に示す５種類又はこれらの組合せが考えられる。

（１）履歴の１行（最新の履歴を除く）を削除
（２）履歴テーブルの最新の履歴を削除
（３）履歴の１行について改変
（４）虚偽の履歴を途中の行の間に挿入
（５）虚偽の履歴を最新の行の後に追加

一方、このようなシステム管理者による履歴テーブル２４の改ざんを不可能とする観点から、システム全体の操作権限を分割する場合がある。この場合、システム操作の権限をもつ管理者と、ネットワーク操作やアプリケーション操作の権限をもつ管理者とを異なる人物に担当させている。しかしながら、この場合でも管理者同士の結託により、履歴テーブル２４が改ざんされる可能性がある。

【００１１】従って、たとえ履歴テーブル２４の操作権限を持つ管理者であっても、履歴テーブル２４の改ざんを不可能とする技術が必要とされている。

【００１２】本発明は上記実情を考慮してなされたもので、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びＩＣカードを提供することを目的とする。

【００１３】

【課題を解決するための手段】第１の発明は、計算機システムの操作の履歴管理を実現するための履歴管理用のコンピュータ読取り可能な記憶媒体であって、前記計算機システムのコンピュータを、前記操作毎に今回の履歴データ及び認証子が追加的に記憶される履歴テーブルを形成するテーブル形成手段、前記操作毎に今回の履歴データ及び前回の認証子に基づいて今回の認証子が生成されると、この今回の認証子を前記今回の履歴データと組にして前記履歴テーブルに記憶させる履歴管理手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。ここで、履歴データは、例えばコマンド、パラメータ及び実行結果の組であり、所望によって以上の組に行番号を含めてもよい。

【００１４】このように、管理者の操作履歴に対する各履歴データ毎に、前回の認証子をも含んで生成した認証子をつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性とを保証でき、もって、管理者による履歴の改ざんを阻止することができる。

【００１５】第２の発明は、第１の発明において、前記計算機システムのコンピュータを、前記履歴テーブル内の各回の履歴データ毎に、当該回の履歴データと当該回の前回の認証子とに基づいて、当該回の認証子が生成されるか否かを定期的に検証する第１の検証手段、前記第２の検証手段により当該回の認証子が生成されないとき、警告を発する第１の警告手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。

【００１６】従って、定期的に第１の発明と同様の作用を奏することができる。

【００１７】第３の発明は、第２の発明において、前記計算機システムのコンピュータを、前記履歴テーブル内の最新の認証子を比較のために出力し、折り返し入力された比較結果を判定する第２の検証手段、前記第２の検証手段による判定結果が不整合を示すとき、警告を発する第２の警告手段、として機能させるためのプログラムが記憶されたコンピュータ読取り可能な記憶媒体である。

【００１８】このように、最新の認証子の比較結果をも検証するので、第２の発明の作用に加え、最新の認証子の削除に関しても、管理者による履歴の改ざんを阻止することができる。

【００１９】第４の発明は、第３の発明において、前記第２の検証手段がログオンのときに動作するコンピュータ読取り可能な記憶媒体である。

【００２０】従って、ログオン時に第３の発明と同様の作用を奏することができる。

【００２１】一方、第５の発明は、電子計算機システムの操作の履歴管理を実現するための履歴管理用のＩＣカ

ードであって、耐タンパー性を有し、最新の認証子が記憶される最新認証子記憶手段と、前記操作毎に今回の履歴データが入力されると、今回の履歴データと前記最新認証子記憶手段内の最新の認証子とに基づいて、今回の認証子を生成する認証子生成手段と、この認証子生成手段により生成された今回の認証子を最新の認証子として前記最新認証子記憶手段に書込む認証子書込手段と、認証子が入力されたとき、この入力された認証子と、前記最新認証子記憶手段内の最新の認証子とを比較し、比較結果を出力する認証子比較手段と、を備えたＩＣカードである。

【００２２】このように、耐タンパー性を有して最新の認証子を保持し、最新の認証子の比較結果を検証するので、最新の履歴に関し、管理者による履歴の改ざんを阻止することができる。

【００２３】第６の発明は、第５の発明において、パスワードによる操作者の認証を実行する操作者認証手段を備え、前記認証子比較手段としては、前記操作者認証手段による認証結果が正当なとき、動作するＩＣカードである。

【００２４】従って、操作者の認証後に第５の発明と同様の作用を奏することができる。

【００２５】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照しながら説明する。

（第１の実施形態）図１は本発明の第１の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図であり、図２はこの計算機システムの構成を示す機能ブロック図であって、前述した図面と同一部分には同一符号を付し、前述した部分を改良した部分にはアルファベットの添字を付して、前述した部分と重複する説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

【００２６】すなわち、本実施形態は、管理者による履歴の改ざんを阻止し得るものであり、具体的には、前述の履歴テーブル２４に代えて、各行毎に認証子Ｃをも記憶する履歴テーブル２４Ａが設けられ、且つこの履歴テーブル２４Ａとコマンド解釈機能２２との間に履歴管理機能２５が設けられ、この履歴管理機能２５がＩＣカードＲ／Ｗ２６を介してＩＣカード３０に接続可能な構成となっている。

【００２７】ここで、履歴テーブル２４Ａは、図３に示すように、前述した履歴テーブル２４に比べ、各操作に対応するコマンド、パラメータ及び実行結果の組毎に認証子Ｃが記録される構成となっている。なお、履歴テーブル２４Ａは、例えば、始めに履歴管理機能２５により初期化されて形成される。

【００２８】認証子Ｃは、前回までの行に記憶された履歴データ（例、コマンド、パラメータ及び実行結果の組）及び認証子Ｃと、今回の行に記憶された履歴データとに密接に関連するデータであり、例えば署名データのように何らかの暗号化データが適用可能となっている。

【００２９】具体的には認証子Ｃは、前回の行の認証子Ｃと、今回の行のコマンド、パラメータ及び実行結果とに関してＩＣカード３０内で秘密鍵を用いた暗号化処理により生成され、ＩＣカードＲ／Ｗ２６及び履歴管理機能２５を介して履歴テーブル２４Ａの該当する行番号の列領域に書込まれる。但し、認証子Ｃの生成方法は、コマンド、パラメータ、実行結果、直前行の認証子Ｃ、及び秘密鍵についての関数であればよく、その生成過程は任意である。

【００３０】例えば、今回のコマンド、パラメータ及び実行結果と、直前行の認証子Ｃとについてのハッシュ値をとり、得られたハッシュ値を秘密鍵で暗号化した値を最新の認証子Ｃとする生成方法や、今回のコマンド、パラメータ及び実行結果の組のハッシュ値を得た後、このハッシュ値と直前行の認証子Ｃとの排他的論理和ＸＯＲをとり、得た結果を秘密鍵で暗号化した値を最新の認証子Ｃとする生成方法などが考えられる。

【００３１】なお、認証子Ｃは、検証時に、履歴を削除・改変・挿入・追加した内容（１），（３）～（５）の改ざんを検知する機能として、（ｆ１）一行毎の履歴が改ざんされてない旨を保証する機能と、（ｆ２）直前の認証子Ｃと関連を有して履歴の連鎖性を保証する機能とを有している。例えば、ある行の履歴を削除した場合、削除した行よりも後の行の認証子Ｃを検証した際に、エラーを発生させる。

【００３２】履歴管理機能２５は、コマンド解釈機能２２と履歴テーブル２４Ａとの間に介在して設けられ、最新の認証子Ｃを更新する更新機能と、認証子の内容を検証する第１の検証機能と、最新の認証子Ｃの削除を検証する第２の検証機能とを有するものである。履歴管理機能２５における更新機能は、コマンド解釈機能２２から受けたコマンド、パラメータ及び実行結果をＩＣカードＲ／Ｗ２６を介してＩＣカード３０に入力し、折り返し、ＩＣカード３０から受けた認証子Ｃと、当該コマンド、パラメータ及び実行結果とを履歴テーブル２４Ａの最後の同一行に書込むものである。

【００３３】履歴管理機能２５における第１の検証機能は、履歴テーブル２４Ａ内の各行毎に、ｋ行目のコマンド、パラメータ及び実行結果と、ｋ－１行目の認証子Ｃとを対象にし、公開鍵を用いて認証子Ｃの生成と逆の操作により、ｋ行目の認証子Ｃを検証するものである。

【００３４】一方、ＩＣカード３０は、図４に示すように、最新認証子格納庫３１、秘密鍵格納庫３２及び制御機能３３を備えている。履歴管理機能２５における第２の検証機能は、履歴テーブル１０の最新の行の認証子Ｃを読出してこの認証子ＣをＩＣカードＲ／Ｗ２６経由で制御機能３３に送る一方、制御機能３３から返信された

比較結果を判定するものである。

【００３５】なお、履歴管理機能２５は、ハードウェア及び／又はソフトウェアにより実現可能であり、ソフトウェアで実現される場合、コンピュータ読取り可能な記憶媒体から履歴管理機能２５に相当するプログラムがインストールされて実現される。これは他の各機能２１～２３についても同様である。

【００３６】最新認証子格納庫３１は、耐タンパー性を有し、外部から一切アクセス不能であって常に最新の認証子Ｃが追加又は更新されて格納される領域であり、制御機能３３により最新の認証子Ｃが読出／書込可能となっている。なお、最新認証子格納庫３１は、最新の行の履歴に対する認証子Ｃを外部から改変不可に保持することにより、履歴テーブル２４Ａにおける最新の履歴を削除する内容（２）の改ざんを阻止する機能（又は改ざん後にそれを検出する機能）を有する。また、最新認証子格納庫３１の認証子Ｃは、初めてＩＣカード３０により管理操作を行う場合には予め定められた初期値Ｃが設定され、以後、新たな認証子Ｃが生成される毎に、最新の認証子Ｃに書換えられる。

【００３７】秘密鍵格納庫３２は、耐タンパー性を有し、外部から一切アクセス不能であってＩＣカード３０の秘密鍵が格納される領域であり、制御機能３３により読出可能となっている。

【００３８】制御機能３３は、最新の認証子を更新する更新機能と、最新の認証子を検証する検証機能とを有する。制御機能３３における更新機能は、履歴管理機能２５からＩＣカードＲ／Ｗ２６を介して、コマンド、パラメータ及び実行結果からなる今回の処理内容を受けたとき、この処理内容を秘密鍵格納庫３１内の秘密鍵で暗号化し、得られた最新の認証子Ｃを最新認証子格納庫３１に書込む一方、この最新の認証子ＣをＩＣカードＲ／Ｗ２６を介して履歴管理機能２５に返信するものである。

【００３９】制御機能３３における検証機能は、履歴管理機能２５からＩＣカードＲ／Ｗ２６を介して受信した認証子Ｃと、最新認証子格納庫３１内の最新の認証子Ｃとを比較し、両者の比較結果をＩＣカードＲ／Ｗ２６を介して履歴管理機能２６に返信するものである。

【００４０】次に、以上のように構成された計算機システムの動作を図５～図７のフローチャートを用いて説明する。

（管理操作）計算機１０は、図５に示すように、管理者の操作により、ＧＵＩ１１により操作内容を指定する（ＳＴ１）。

【００４１】この操作内容は、コマンド発行機能１２によりコマンドとパラメータとを含む形式のコマンド電文に変換され、このコマンド電文がソケット１３を経由してサーバ装置２０Ａに送信される（ＳＴ２）。

【００４２】サーバ装置２０Ａでは、コマンド電文がソケット２１を経由してコマンド解釈機能２２に入力され、コマンド解釈機能２２によりコマンド電文からコマンドとパラメータが取り出される（ＳＴ３）。

【００４３】また、コマンド解釈機能２２は、コマンドに対応する管理機能２３を実行し、実行結果を管理機能２３から受け取る（ＳＴ４）。

【００４４】次に、コマンド解釈機能２２は、コマンド、パラメータ及び実行結果を履歴管理機能２５に入力する（ＳＴ５）。履歴管理機能２５は、コマンド、パラメータ及び実行結果をＩＣカードＲ／Ｗ２６を経てＩＣカード３０に入力する（ＳＴ６）。

【００４５】ＩＣカード３０では、制御機能３３が、これら入力された今回のコマンド、パラメータ及び実行結果と、最新認証子格納庫３１の前回の認証子Ｃとに対し、秘密鍵格納庫３２内の秘密鍵による暗号化を施して最新の認証子Ｃを生成する（ＳＴ７）。

【００４６】ＩＣカード３０は、最新の認証子Ｃを最新認証子格納庫３１に格納し（ＳＴ８）、この最新の認証子ＣをＩＣカードＲ／Ｗ２６を通して履歴管理機能２５に返す（ＳＴ９）。履歴管理機能２５は、コマンド、パラメータ及び実行結果と最新の認証子Ｃとを履歴テーブル２４Ａに書込む（ＳＴ１０）。

【００４７】履歴テーブル２４Ａへの書込完了後、コマンド解釈機能２２は、実行結果を計算機１０に返すためのレスポンス電文を生成し、ソケット２１を経由して計算機１０に返信する（ＳＴ１１）。

【００４８】計算機１０は、このレスポンス電文を受信し、ＧＵＩ１１により実行結果を表示して今回の操作を終了する（ＳＴ１２）。

【００４９】（履歴の検証）以上のように記録された履歴テーブル２４Ａは、履歴管理機能２５による認証子Ｃの検証により、履歴の改ざんの有無が定期的に調べられる。なお、検証の際には、履歴テーブル２４Ａの各行毎に認証子Ｃが正当（＝各行の連鎖及び生成が正当）であるか否かの履歴の検証と、最新の認証子ＣとＩＣカード内の認証子Ｃとが同一であるか否かの最新履歴の検証とが実行される。以下、詳しく説明する。

【００５０】始めに、履歴管理機能２５は、図６に示すように、履歴テーブル２４Ａ内の行番号ｋを定め、ｋ＝１とする（ＳＴ２１）。次に、履歴管理機能２５は、履歴テーブル２４Ａのｋ行目のコマンド、パラメータ、実行結果及び認証子Ｃを読み出し（ＳＴ２２）、行番号ｋ＝１であるか否かを判定する（ＳＴ２３）。

【００５１】行番号ｋ＝１の場合には、履歴テーブル２４Ａ内のｋ－１行目が無いため、直前行の認証子Ｃとして予め定めた初期値を入れる（ＳＴ２４）。

【００５２】行番号ｋ≠１の場合には、履歴テーブル２４Ａ内のｋ－１行目の認証子Ｃを読み出す（ＳＴ２５）。

【００５３】ステップＳＴ２４又はＳＴ２５の後、ｋ行目のコマンド、パラメータ及び実行結果と、ｋ－１行目

の認証子Ｃと、公開鍵とを用いてｋ行目の認証子Ｃを検証する（ＳＴ２６）。この検証は、認証子Ｃの生成方法と逆の操作で実行可能であり、その検証方法自体は任意である。

【００５４】例えば、ｋ行目のコマンド、パラメータ及び実行結果と、ｋ－１行目の認証子Ｃとについてのハッシュ値をとり、得られたハッシュ値と認証子Ｃを公開鍵で復号した値が等しいか否かを調べる検証方法や、ｋ行目のコマンド、パラメータ及び実行結果のハッシュ値を得た後、このハッシュ値とｋ－１行目の認証子Ｃとの排他的論理和ＸＯＲをとり、その結果と認証子Ｃを公開鍵で復号したものが等しいか調べる検証方法などが考えられる。

【００５５】ステップＳＴ２６の検証に基づき、ｋ行目の認証子Ｃを正当か否かを判定し（ＳＴ２７）、ｋ行目の認証子Ｃを正当であると判定したとき、履歴の最後の行まで検証したか否かを判定し（ＳＴ２８）、最後の行まで検証してない場合には行番号ｋを１行分増加し（ＳＴ２９）、ステップＳＴ２２に戻って同様の操作を繰り返す。なお、ステップＳＴ２８にて最後の行まで検証した場合には検証処理を終了する。

【００５６】一方、ステップＳＴ２７にて、ｋ行目の認証子Ｃを正当でないと判定したとき、警告を発して（ＳＴ３０）、検証処理を終了する。

【００５７】以上により、１行目から最後の行までの履歴に関し、各行の認証子が同一行のコマンド、パラメータ及び実行結果を含んで生成されることから各行毎に改ざんされていない旨と、各行の認証子が直前行の認証子を含んで生々されることから各行の履歴が連鎖している旨とが検証される。但し、図６に示した検証では、最後の行（最新履歴）が削除されたか否かは検証されない。よって、次に、この最新履歴の検証に関して述べる。なお、最新履歴の検証は、前述した履歴の検証において、各行の認証子Ｃが全て正当と判定された場合に実行される。

【００５８】（最新履歴の検証）履歴管理機能２５は、図７に示すように、履歴テーブル２４Ａの最新の行の認証子Ｃを読出すと共に（ＳＴ３１）、この認証子ＣをＩＣカードＲ／Ｗ２６を介してＩＣカード３０に送る（ＳＴ３２）。

【００５９】ＩＣカード３０では、制御機能３３がサーバ装置２０Ａから送られた認証子Ｃと、最新認証子格納庫３１内の最新の認証子Ｃとを比較し、比較結果をＩＣカードＲ／Ｗ２６を経由してサーバ装置２０Ａの履歴管理機能２５に送る（ＳＴ３３）。

【００６０】履歴管理機能２５は、比較結果が両認証子Ｃの同一を示すか否かを判定し（ＳＴ３４）、判定結果が同一を示すときに処理を終了する。同一でない場合は警告を発し（ＳＴ３５）、処理を終了する。

【００６１】上述したように本実施形態によれば、管理者の操作履歴に対する各履歴データ（例、コマンド、パラメータ及び実行結果の組）毎に、前回の認証子をも含んで生成した認証子をつけるので、履歴データが改ざんされていない旨と、個々の履歴データの連鎖性とを保証でき、もって、管理者による履歴の改ざんを阻止することができる。

【００６２】また、最新の認証子の比較結果をも検証するので、最新の認証子の削除に関しても、管理者による履歴の改ざんを阻止することができる。

【００６３】また、今回の認証子を生成する際に、以前の履歴を代表するデータとして前回の認証子を用いるので、以前の全ての履歴データを用いて今回の認証子を計算する場合と比べ、ファイルが膨大になることを阻止できると共に、計算量を低下させて認証子の生成速度を向上させることができる。

【００６４】なお、本実施形態は、ＩＣカード３０内に認証子を格納し、ＩＣカード自体は管理者ですら内容を改ざんできない耐タンパー機構とすることにより、履歴の改ざんを防止している。但し、サーバ装置２０ＡにＩＣカードＲ／Ｗ２６を接続することから、ＩＣカード３０の管理を厳密にする必要がある。

【００６５】（第２の実施形態）図８は本発明の第２の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図であり、図９はこの計算機システムの構成を示す機能ブロック図である。

【００６６】本実施形態は、第１の実施形態の変形例であり、ＩＣカードＲ／Ｗ１４を計算機１０Ａのコマンド発行機能１２Ａに接続し、この計算機１０Ａ側において最新履歴の検証機能を行なう構成となっている。

【００６７】コマンド発行機能１２Ａは、前述したＧＵＩ１１１の操作に基づきコマンド電文を作成する機能に加え、認証子の生成に関する第１の中継機能と、最新の認証子Ｃの検証に関する第２の中継機能とをもっている。

【００６８】コマンド発行機能１２Ａにおける第１の中継機能は、サーバ装置２０Ｂから受けたレスポンス電文から実行結果を取り出す機能と、この実行結果と、コマンド電文を作成した際のコマンド及びパラメータとをＩＣカードＲ／Ｗ１４を経由してＩＣカード３０Ａに入力する機能と、ＩＣカード３０ＡからＩＣカードＲ／Ｗ１４を経由して最新の認証子Ｃを受けると、この最新の認証子Ｃを含む認証子電文を生成し、この認証子電文をソケット１３経由でサーバ装置２０Ｂに送る機能とから構成されている。

【００６９】コマンド発行機能１２Ａにおける第２の中継機能は、サーバ装置２０Ｂから受けた認証子電文から認証子Ｃを取り出す機能と、この認証子ＣをＩＣカードＲ／Ｗ１４経由でＩＣカード３０Ａに入力する機能と、ＩＣカード３０AからＩＣカードＲ／Ｗ１４経由で受けた比較結果をソケット１３経由でサーバ装置２０Ｂに送

る機能とから構成されている。

【００７０】履歴管理機能２５Ａは、前述した機能において、ＩＣカードＲ／Ｗ２６に対する送受信に代えて、ＩＣカード３０Ａに対するコマンド、パラメータ、実行結果及び認証子の送信や最新の認証子の受信を、計算機１０Ａを介して行なう構成となっている。なお、この履歴管理機能２５Ａも記憶媒体からプログラムがインストールされることにより実現可能となっている。

【００７１】ＩＣカード３０Ａは、前述した各機能に加え、管理者の認証を行なうための認証機能３４を備えている。認証機能３４は、ＩＣカード３０ＡがＩＣカードＲ／Ｗ１４に挿入されたとき、管理者の操作により、管理者の認証を実行する機能と、この実行結果が管理者の正当な旨を示すとき、履歴管理機能２５Ａに対して最新履歴の検証を実行させる機能とをもっている。なお、管理者の認証としては、例えばパスワードによる認証といった周知の認証方式が使用可能となっている。

【００７２】次に、以上のように構成された計算機システムの動作を図１１～図１３を用いて説明する。

（管理操作）始めに、計算機１０Ａでは、管理者の操作に対し、ＩＣカード３０Ａの認証機能３４を用いて認証を行なう。管理者の認証の後、後述する最新履歴の検証が正常に完了すると、計算機システムは、図１１及び図１２に示す如き、管理操作が可能となる。

【００７３】いま、計算機１０Ａの管理操作からサーバ装置２０Ｂのコマンド実行までは、図１２に示すように、前述同様に実行される（ＳＴ１～ＳＴ４）。サーバ装置２０Ｂでは、コマンド解釈機能２２が、管理機能２３の返す実行結果をもとにコマンド解釈機能２２においてレスポンス電文を生成し、当該レスポンス電文をソケット２１を介して計算機１０Ａに送信する（ＳＴ４１）。

【００７４】計算機１０Ａでは、このレスポンス電文をソケット１３を経由してコマンド発行機能１２Ａが受け、コマンド発行機能１２Ａがレスポンス電文から実行結果を取り出す（ＳＴ４２）。

【００７５】また、コマンド発行機能１２Ａは、コマンド電文を生成した際のコマンド及びパラメータと、レスポンス電文から取り出した実行結果とをＩＣカードＲ／Ｗ１４を経由してＩＣカード３０Ａに入力する（ＳＴ４３）。

【００７６】ＩＣカード３０Ａは、これらの入力内容に対し、秘密鍵格納庫３２内の秘密鍵による暗号化を施して前述同様に最新の認証子Ｃを生成し、この最新の認証子Ｃを最新認証子格納庫３１に格納する一方（ＳＴ４４）、この最新の認証子ＣをＩＣカードＲ／Ｗ１４を介してコマンド発行機能１２Ａに出力する。

【００７７】コマンド発行機能１２Ａは、ＩＣカード３０Ａから受けた最新の認証子Ｃを含む認証子電文を生成し、この認証子電文をソケット１３経由でサーバ装置２０Ｂに送り返す（ＳＴ４５）。

【００７８】サーバ装置２０Ｂでは、認証子電文をソケット２１経由でコマンド解釈機能２２にて受け取り、認証子Ｃを取り出す。

【００７９】コマンド解釈機能２２は、ステップＳＴ４のコマンド、パラメータ及び実行結果と、計算機１０Ａから受けた最新の認証子Ｃとを履歴管理機能２５Ａに送る。履歴管理機能２５Ａは、これらコマンド、パラメータ、実行結果及び最新の認証子Ｃを履歴テーブル２４Ａに書込んで（ＳＴ４６）、処理を終了する。

【００８０】（履歴の検証）履歴テーブル２４Ａの各行毎の認証子Ｃに対する検証は、第１の実施形態と同様に実行される。この検証の実行タイミングは任意である。

【００８１】（最新履歴の検証）最新の認証子ＣとＩＣカード３０Ａ内の認証子Ｃの検証について図１３のフローチャートを用いて説明する。この検証は、ＩＣカード３０Ａを管理者が保持するために、任意のタイミングでは実行されない。そこで、この検証は、例えば管理者がサーバ装置２０Ｂにログインした時（認証機能３４による認証の直後）といった特定のタイミングに実行される。なお、この検証は、前述した図７に示す検証において、履歴管理機能２５ＡとＩＣカード３０Ａとの間に計算機１０Ａを介在させたものである。

【００８２】始めに、サーバ装置２０Ｂでは、履歴管理機能２５Ａが履歴テーブル２４Ａの最新の行の認証子Ｃを読出すと共に（ＳＴ５１）、この認証子Ｃをコマンド解釈機能２２に与える。コマンド解釈機能２２は、この認証子Ｃを認証子電文の形でソケット２１を介して計算機１０Ａに送る（ＳＴ５２）。

【００８３】計算機１０Ａでは、認証子電文をコマンド発行機能１２Ａで受け取り、認証子ＣをＩＣカード３０Ａに送る（ＳＴ５３）。

【００８４】ＩＣカード３０Ａでは、制御機能３３がサーバ装置２０Ａから送られた認証子Ｃと、最新認証子格納庫３１内の認証子Ｃとを比較し、比較結果をＩＣカードＲ／Ｗ１４を経由して計算機１０Ａのコマンド発行機能１２Ａに返す（ＳＴ５４）。

【００８５】コマンド発行機能１２Ａは、比較結果をソケット１３を介してサーバ装置２０Ｂに送る（ＳＴ５５）。

【００８６】サーバ装置２０Ｂでは、比較結果を履歴管理機能２５Ａが受取り、この履歴管理機能２５Ａが、比較結果について両認証子Ｃの同一を示すか否かを判定し（ＳＴ５６）、判定結果が同一を示すときに処理を終了する。同一でない場合は警告を発し（ＳＴ５７）、処理を終了する。

【００８７】この処理が例えばログイン時に行われたとき、計算機１０Ａは、以後の管理操作が可能となる。

【００８８】上述したように本実施形態によれば、ＩＣカード３０ＡをＩＣカードＲ／Ｗ１４を介して計算機１

０Ａに接続し、計算機１０Ａ側において最新履歴の検証を実行させる構成としても、第１の実施形態と同様の効果を得ることができる。

【００８９】なお、第２の実施形態は、ＩＣカード３０Ａを管理者側の管理とし、管理者のシステムへの認証を兼ねている構成である。しかし、計算機１０Ａとサーバ装置２０Ｂの間の通信が中断した場合、ＩＣカード３０Ａ内の最新の認証子Ｃと、サーバ装置２０Ｂ側の最新の認証子Ｃとが不整合となる可能性がある。この場合、履歴改ざんの警告が出されるが、この警告が改ざんによるものか、通信の中断によるものかの判断が困難である。このため、第２の実施形態は、通信上のトラブルの可能性が低い、あるいは別の手段でトラブルが回避できる状況のときに用いることが好ましい。

【００９０】尚、本発明における記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【００９１】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【００９２】さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【００９３】また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【００９４】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【００９５】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【００９６】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。

【００９７】例えば、計算機１０に代えて、計算機１０，１０Ａと同一構成のコンソール１０＊，１０Ａ＊をサーバ装置２０Ａ，２０Ｂに接続し、このコンソール１０＊，１０Ａ＊からサーバ装置２０Ａ，２０Ｂを管理する構成としても、本発明を同様に実施して同様の効果を得ることができる。

【００９８】ＩＣカードＲ／Ｗ２６は、外付けの態様に限らず、サーバ装置２０に内蔵された態様としてもよい。ＩＣカードＲ／Ｗ１４も同様に計算機１０Ａに内蔵されていてもよい。また、ＩＣカード３０，３０Ａは、同様の機能を有し、内部のデータが安全に管理されるデバイス（例、ＩＣカードと同様の機能をもつ回路が形成されたボードなど）に変更してもよく、この場合、ＩＣカードＲ／Ｗ２６，１４は省略してもよい。

【００９９】また、各実施形態は可能な限り適宜組合せて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組合せにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【０１００】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【０１０１】

【発明の効果】以上説明したように本発明によれば、管理者による履歴の改ざんを阻止し得る履歴管理用の記憶媒体及びＩＣカードを提供できる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図

【図２】同実施形態における計算機システムの構成を示す機能ブロック図

【図３】同実施形態における履歴テーブルの構成を示す模式図

【図４】同実施形態におけるＩＣカードの構成を示す機能ブロック図

【図５】同実施形態における動作を説明するためのフローチャート

【図６】同実施形態における動作を説明するためのフローチャート

【図７】同実施形態における動作を説明するためのフローチャート

【図８】本発明の第２の実施形態に係る記憶媒体内のプログラムがインストールされた計算機システムの概略を示す模式図

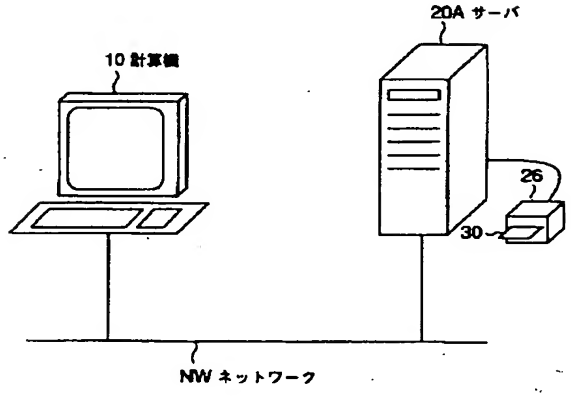
【図９】同実施形態における計算機システムの構成を示す機能ブロック図

【図１０】同実施形態におけるＩＣカードの構成を示す機能ブロック図

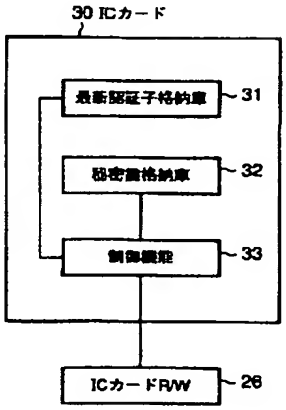
【図１１】同実施形態における動作を説明するためのシ

ーケンス図
【図１２】同実施形態における動作を説明するためのフローチャート
【図１３】同実施形態における動作を説明するためのフローチャート
【図１４】従来の計算機システムの概略を示す模式図
【図１５】従来の計算機システムの構成を示す機能ブロック図
【図１６】従来の履歴テーブルの構成を示す模式図
【符号の説明】
１０，１０Ａ…計算機
１１…ＧＵＩ
１２，１２Ａ…コマンド発行機能
１３，２１…ソケット
１４，２６…ＩＣカードＲ／Ｗ
２０Ａ，２０Ｂ…サーバ装置
２２…コマンド解釈機能
２３…管理機能
２４Ａ…履歴テーブル
２５，２５Ａ…履歴管理機能
３０，３０Ａ…ＩＣカード
３１…最新認証子格納庫
３２…秘密鍵格納庫
３３…制御機能
３４…認証機能
ＮＷ…ネットワーク
Ｃ…認証子

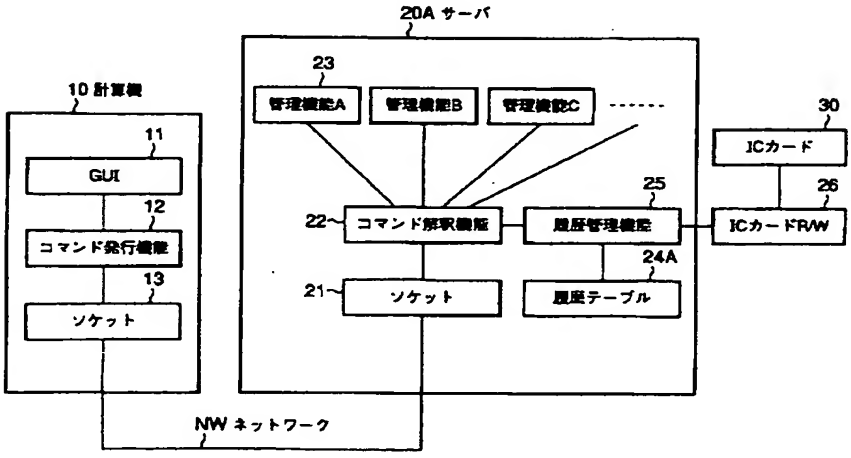
【図１】



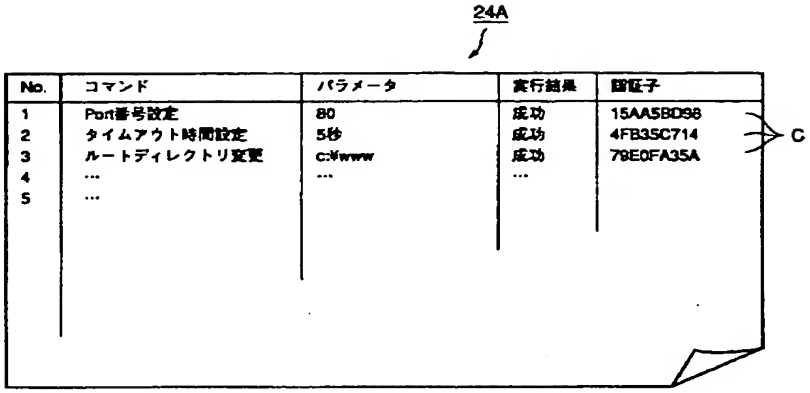
【図４】



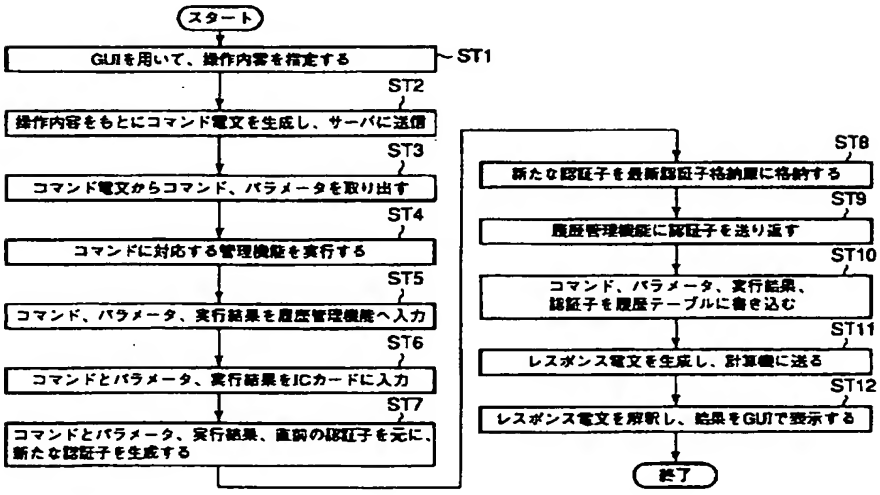
【図２】



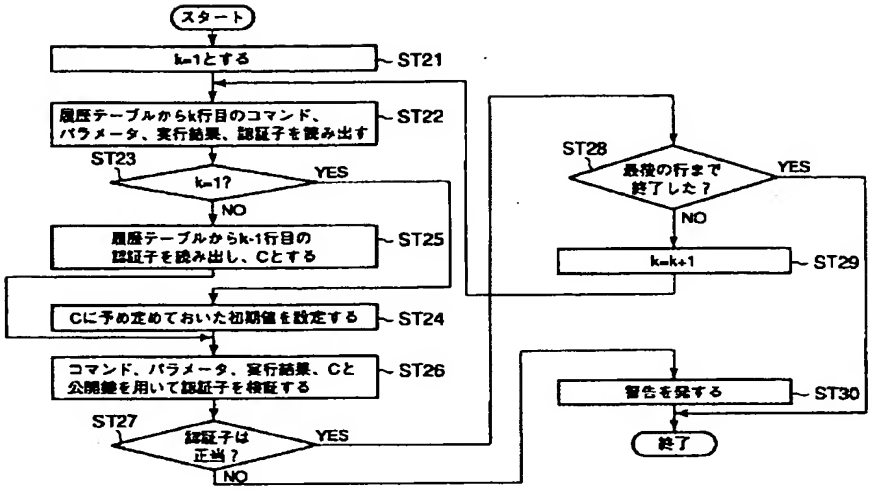
【図３】


24A
No.
コマンド
パラメータ
実行結果
認証子
1
Port番号設定
80
成功
15AA5BD98
2
タイムアウト時間設定
5秒
成功
4FB35C714
3
ルートディレクトリ変更
c:¥www
成功
79E0FA35A
4
…
…
…
5
…
C

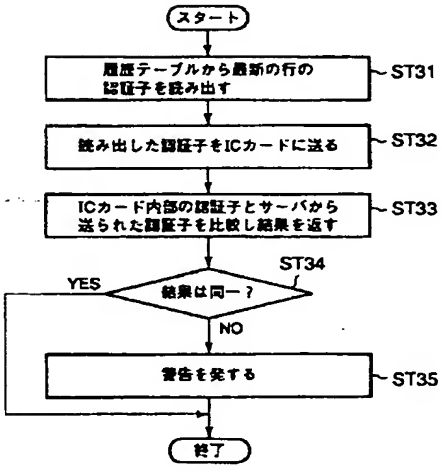
【図５】


スタート
GUIを用いて、操作内容を指定する
ST1
ST2
操作内容をもとにコマンド電文を生成し、サーバに送信
ST3
コマンド電文からコマンド、パラメータを取り出す
ST4
コマンドに対応する管理機能を実行する
ST5
コマンド、パラメータ、実行結果を履歴管理機能へ入力
ST6
コマンドとパラメータ、実行結果をICカードに入力
ST7
コマンドとパラメータ、実行結果、直前の認証子を元に、新たな認証子を生成する
ST8
新たな認証子を最新認証子格納部に格納する
ST9
履歴管理機能に認証子を送り返す
ST10
コマンド、パラメータ、実行結果、認証子を履歴テーブルに書き込む
ST11
レスポンス電文を生成し、計算機に送る
ST12
レスポンス電文を解釈し、結果をGUIで表示する
終了

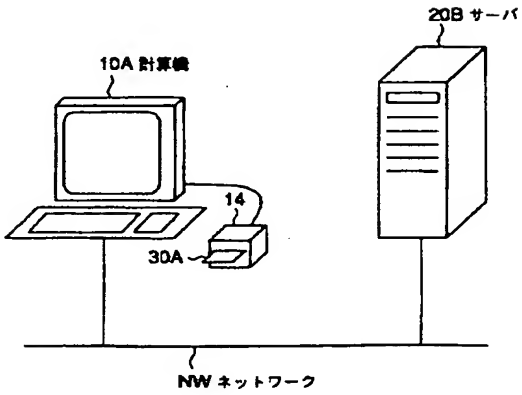
【図６】


スタート
k=1とする
ST21
履歴テーブルからk行目のコマンド、パラメータ、実行結果、認証子を読み出す
ST22
ST23
k=1?
YES
NO
履歴テーブルからk-1行目の認証子を読み出し、Cとする
ST25
Cに予め定めておいた初期値を設定する
ST24
コマンド、パラメータ、実行結果、Cと公開鍵を用いて認証子を検証する
ST26
ST27
認証子は正当？
YES
NO
ST28
最後の行まで終了した？
YES
NO
k=k+1
ST29
警告を発する
ST30
終了

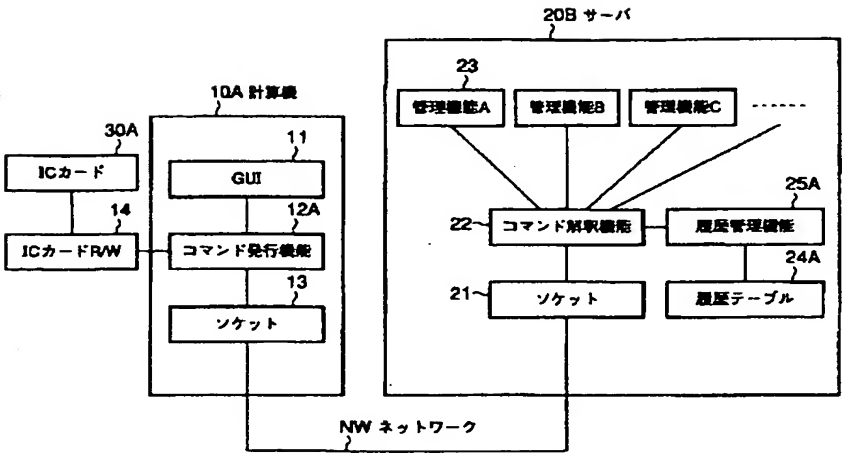
【図７】


スタート
履歴テーブルから最新の行の認証子を読み出す
ST31
読み出した認証子をICカードに送る
ST32
ICカード内部の認証子とサーバから送られた認証子を比較し結果を返す
ST33
ST34
YES
結果は同一？
NO
警告を発する
ST35
終了

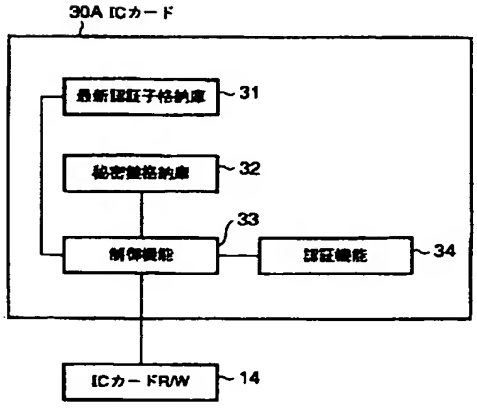
【図８】


20B サーバ
10A 計算機
14
30A
NW ネットワーク

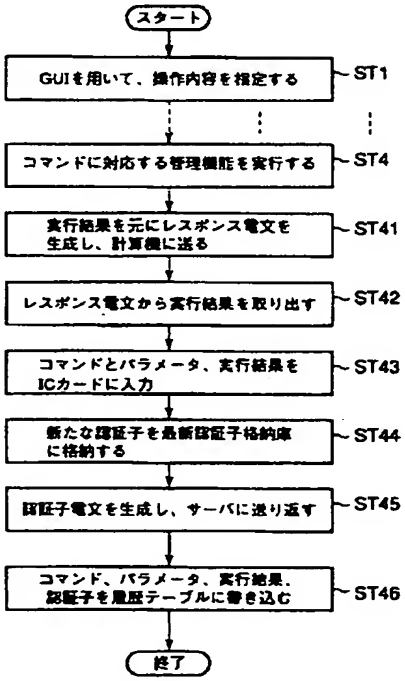
【図９】


20B サーバ
23
管理機能A
管理機能B
管理機能C
10A 計算機
30A
11
ICカード
GUI
25A
14
12A
22
コマンド解釈機能
履歴管理機能
ICカードR/W
コマンド発行機能
24A
13
21
ソケット
履歴テーブル
ソケット
NW ネットワーク

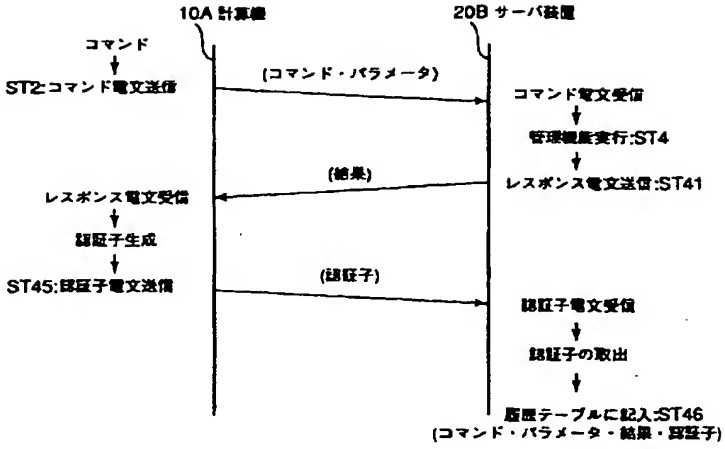
【図１０】


30A ICカード
最新認証子格納庫
31
秘密鍵格納庫
32
33
制御機能
認証機能
34
ICカードR/W
14

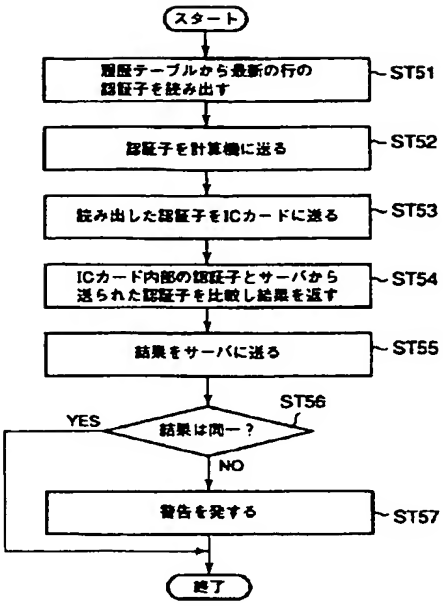
【図１２】


スタート
GUIを用いて、操作内容を指定する
ST1
コマンドに対応する管理機能を実行する
ST4
実行結果を元にレスポンス電文を生成し、計算機に送る
ST41
レスポンス電文から実行結果を取り出す
ST42
コマンドとパラメータ、実行結果をICカードに入力
ST43
新たな認証子を最新認証子格納庫に格納する
ST44
認証子電文を生成し、サーバに送り返す
ST45
コマンド、パラメータ、実行結果、認証子を履歴テーブルに書き込む
ST46
終了

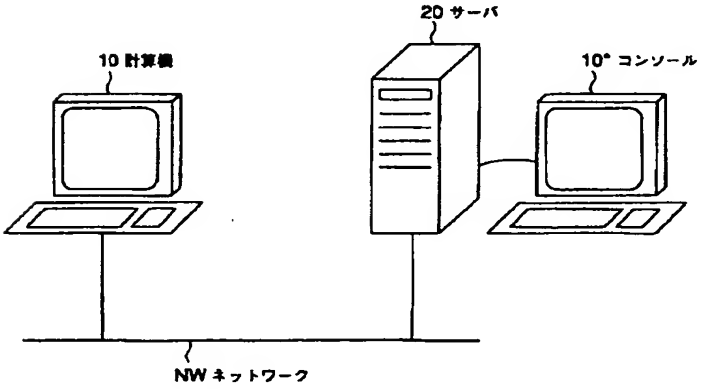
【図１１】



【図１３】



【図１４】

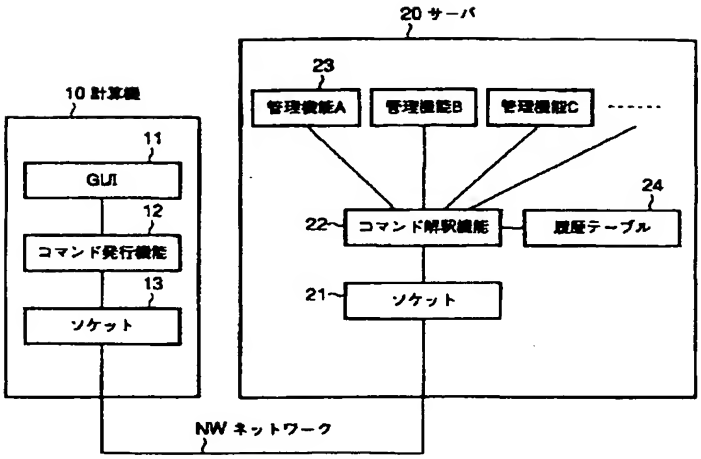


【図１６】

24

No.	コマンド	パラメータ	実行結果
1	Port番号設定	80	成功
2	タイムアウト時間設定	5秒	成功
3	ルートディレクトリ変更	c:¥www	成功
4	…	…	
5	…		

【図１５】



フロントページの続き

Ｆターム(参考) 5B017 AA01 BA06 BB09 CA15 CA16
5B035 AA13 BB09 BC00 CA38
5B042 JJ08 JJ10 KK13 MA20 MC37
MC40
5J104 AA08 BA02 LA03 LA05 NA02
NA12 NA31 NA32 NA35 NA37
NA38 NA42